AF
ZW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Baiju V. Patel et al.	§	Group Art Unit:	2135
Serial No.:	09/364,835	§	Examiner:	Leynna A. Ha
Filed:	July 30, 1999	§	Assignee:	Intel Corporation
For:	Technique And Apparatus For Processing Cryptographic Services Of Data In A Network System	§	Atty. Dkt. No.:	ITL.0182US (P6867)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF TRANSMITTAL

Dear Sir:

Transmitted herewith is the Appeal Brief in this application. The Notice of Appeal was filed on October 10, 2005.

Pursuant to M.P.E.P. § 1208.02, there is no fee due for this Appeal, because the Examiner reopened prosecution after filing of the first Appeal Brief on February 5, 2004. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 20-1504 (ITL.0182US).

Respectfully submitted,

Date: January 20, 2006

Fred G. Pruner, Jr., Reg. No. 40,779
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, Texas 77024
(713) 468-8880 [Phone]
(713) 468-8883 [Fax]
Attorney for Intel Corporation

Date of Deposit: January 20, 2006
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to Mail Stop Appeal Briefs-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Janice Munoz

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Baiju V. Patel et al.	§	Group Art Unit:	2135
Serial No.:	09/364,835	§	Examiner:	Leynna A. Ha
Filed:	July 30, 1999	§	Assignee:	Intel Corporation
For:	Technique And Apparatus For Processing Cryptographic Services Of Data In A Network System	§	Atty. Dkt. No.:	ITL.0182US (P6867)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Date of Deposit: January 20, 2006
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Janice Munoz

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is the assignee Intel Corporation.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-5, 13-20 and 28-37 have been finally rejected and the subject of this appeal.

STATUS OF AMENDMENTS

All amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

At this point, no issue has been raised that would suggest that the words in the claims have any meaning other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

The method of independent claim 1 is for use in a device that is coupled to a communications channel. The method includes determining a security service to perform with a data block and generating security information to pass along with the data block. The security information identifies the security service. The method includes using a computer peripheral device that is adapted to control communication with the communications channel to select the security service from other security services based on the security information that is passed along with the data block. The method includes processing, in the computer peripheral device, the data block according to the security information.

The specification sets forth in an embodiment, a system 50, a network controller 52 and a network 47. The network controller 52 is an example of a computer peripheral device, and the network 47 is an example of a communications channel. The system 50 executes an IP security routine 411 that determines a security service to perform with a data block (an IPSEC packet, for example). More particularly, the specification describes that the IP security routine 411 identifies algorithms to be used for encryption/decryption, authentication and so forth. Specification, 11.

The IP security routine 411 determines whether the security processing is to be offloaded to the network controller 52. Specification, 12. If offloading is desired, then the IP security routine 411 places information in the header portion of an IPSEC packet to indicate the types of algorithms to use for encryption and/or authentication, etc. Specification, 12. Thus, the IP security routine 411 generates security information to pass along with a data block, and the security information identifies a security service to perform with the data block. *Id.*

The network controller 52 is adapted to control communication with the network 47. For the case in which security processing is offloaded to the network controller 52, the network controller 52 selects a security service from other security services based on the security information that is passed along with the data block. For example, on page 18 of the specification, the specification describes that the network controller 52 selects and processes the data for encryption and authentication based on the type or types of algorithms to be employed,

as indicated in the IPSEC packet. Specification, 18. Thus, the specification describes an embodiment of using a computer peripheral device adapted to control communication with the communications channel to select a security service from other security services based on security information and process, in the computer peripheral device, the data block according to the security information. *Id.*

As examples of security services, the specification sets forth such encryption algorithms as block or stream ciphers, public key algorithms and others. As examples of authentication algorithms, the specification sets forth keyed message authentication codes (MACs) based on symmetric encryption algorithm such as the data encryption standard (DES); one-way hash function such as a message digest function (MD5) and a secure hash algorithm (SHA). Specification, 18.

The article of independent claim 13 includes a machine-readable storage medium that contains instructions for execution in a system that includes a computer peripheral device that is adapted to control communications with a communications channel. The instructions when executed cause the system to receive a data block from a computer peripheral device and determine from information in the data block if a security service has been performed on the data block by the computer peripheral device. The instructions cause the system to process the data if the security service has not been performed on the data block by the computer peripheral device.

The specification describes a driver security routine 410 that is executed by the system 50 to, among its other functions, determine if a packet that is received from the network controller 52 has been "punted." Specification, 13. In this regard, if the network controller 52 decides not to process the security information, the network controller 52 marks the packet as "punted" and passes the incoming packet over a system bus interface 131 to the security routine 410. Specification, 20. The security routine 410 then further processes the packet by either passing the packet to the IP security routine 411, which is executed on the system 50, or sending the packet back to the network controller 52. Specification, 13.

Thus, the specification discloses an embodiment of a machine-readable storage medium that contains instructions to cause a system to receive a data block from a computer peripheral device, determine from information in the data block if a security service has been performed on the data block by the computer peripheral device and process the data block if the security service has not been performed on the data block by the computer peripheral device. *Id.*

The controller of independent claim 16 is for controlling communications with a transport medium and includes a receiving circuit and a cryptographic engine. The receiving circuit receives data and associated security control information that identifies a security service to be performed on the data. The controller also includes a cryptographic engine to select the security service from other security services based on the security control information and cryptographically process the data based on the selection.

The specification describes a bus interface 130 and a transmit first in first out (FIFO) queue 122 of the network controller 52 to receive data and associated security control information that identifies the security service to be performed on the data. Specification, 18. A cryptographic engine 126 of the network controller 52 selects a security service from other security services based on security control information associated with the received data and cryptographically processes the data based on the selection. *Id.*

The method of independent claim 28 is for use in a device that is coupled to a communications channel. The method includes determining a security service to perform with a data block and generating security information to pass along with the data block. The security information identifies at least one of an encryption algorithm and an authentication algorithm to be performed by the security service. The method includes processing, in a computer peripheral device that is adapted to control communication with the communications channel, the data block according to the security information.

See discussion of independent claim 1. In particular, the specification sets forth an embodiment in which the IP security routine 411 determines a cryptographic or an authentication algorithm to be performed on an IPSEC packet. Specification, 11. The IP security routine 411 generates security information to pass along with the data block that identifies the encryption and/or authentication algorithm to be performed by the security service. Specification, 11-12. For example, the IP security routine 411 may store this information in the header portion of the IPSEC packet. Specification, 12.

The specification also describes an embodiment in which the network controller 52, a computer peripheral device that is adapted to control communication with the communications channel, processes the IPSEC packet according to the security information. Specification, 13. In particular, the specification describes the network controller 52 performing processing based on

the security control information that identifies encryption and/or authentication algorithms, etc. Specification, 13.

Independent claim 33 recites a controller for controlling communications with a transport medium. The controller includes a receiving circuit and a cryptographic engine. The receiving circuit receives data and associated control information. The security control information identifies at least one of an encryption algorithm and an authentication algorithm to be performed on the data. The cryptographic engine cryptographically processes the data based on the security control information, and the cryptographic engine is a computer peripheral device.

Examples for the elements of claim 33 are set forth above in the discussion of claim 16. In particular, the specification describes a bus interface 130 and transmit FIFO queue 122 of the network controller 52, which constitute an embodiment of the receiving circuit. The network controller 52 also includes a cryptographic engine 126 that cryptographically processes receive data based on security control information that identifies at least one of an encryption algorithm and an authentication algorithm to be performed on the data. The cryptographic engine is a computer peripheral device. Specification, 18.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Are Claims 1-7, 16-20 and 28-37 Anticipated by U.S. Patent No. 5,546,463 (Caputo)?

B. Are Claims 13-15 Anticipated by U.S. Patent No. 5,268,962 (Abadi)?

ARGUMENT

A. Are Claims 1-7, 16-20 and 28-37 Anticipated by U.S. Patent No. 5,546,463 (Caputo)?

The method of independent claim 1 is for use in a device that is coupled to a communications channel. The method includes determining a security service to perform with a data block and generating security information to pass along with the data block. The security information identifies the security service. The method includes using a computer peripheral device that is adapted to control communication with the communications channel to select the security service from other security services based on the security information that is passed along with the data block. The method includes processing, in the computer peripheral device, the data block according to the security information.

Independent claim 1 stands rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,546,463 (herein called "Caputo"). Caputo generally describes a modem, or device 10, which may be connected between a telephone system and a personal computer or terminal. Caputo, 4:54-64. The device 10 performs data encryption and authentication. More specifically, Caputo states that plaintext data 72 is encrypted using a plurality of encryption algorithms and states that the cryptographic algorithms may be chosen from a variety of standard algorithms. Caputo, 5:44-50. Caputo also describes authenticating data by a plurality of authentication algorithms. Caputo, 6:7-9. Caputo also describes a verification process that depends on the algorithm chosen to implement its invention. Caputo, 6:18-20.

The method of independent claim 1 recites generating security information that identifies a security service to perform with a data block so that this information is passed along with the data block. Independent claim 1 also recites using a computer peripheral device to select the security service based on the security information and process the data block according to the security information.

Caputo fails to anticipate independent claim 1 for at least the reason that there is no teaching or suggestion in Caputo regarding generating security information that is passed along with a data block, which identifies a security service to be performed on the data such that a computer peripheral device processes the data block according to the security information. Thus, although at some point during the design of Caputo's device, particular cryptographic and authentication algorithms are chosen for Caputo's device, there is no teaching or suggestion in Caputo that security information is passed along with a data block to be processed by the security

service, which identifies a security service. Additionally, there is no teaching or suggestion in Caputo regarding a computer peripheral device that *selects* a security service among a plurality of security services based on security information that is passed along with a data block. (*emphasis added*). For at least any of these reasons, Caputo fails to anticipate independent claim 1.

The controller of independent claim 16 is for controlling communications with a transport medium and includes a receiving circuit and a cryptographic engine. The receiving circuit receives data and associated security control information that identifies a security service to be performed on the data. The controller also includes a cryptographic engine to select the security service from other security services based on the security control information and cryptographically process the data based on the selection.

Independent claim 16 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Caputo. Caputo fails to anticipate independent claim 16 for at least the reason that Caputo fails to disclose the receiving circuit of this claim.

More specifically, the controller of independent claim 16 recites that the receiving circuit receives data and associated security control information that identifies a security service to be performed on the data. There is no teaching or even a suggestion in Caputo regarding a receiving circuit that receives data and security control information that is associated with this data, where the security control information identifies a security service to be performed on the data. Thus, although Caputo's modem 10 may arguably be programmed with a particular security and/or authentication algorithm, there is no teaching or suggestion of the receiving circuit of independent claim 16.

Caputo fails to anticipate claim 16 for at least the additional, independent reason that Caputo fails to teach the cryptographic engine of claim 16. In this regard, claim 16 recites that the cryptographic engine selects the security service from other security services based on the security control information. Although the designer of the device 10 of Caputo may arguably select a particular security service and configure Caputo's device 10 accordingly, there is no teaching or suggestion in Caputo regarding a cryptographic engine that selects a security service from other security services based on security control information that is received by a receiving circuit and is associated with received data that is processed pursuant to the selected security

service. Therefore, for at least this additional, independent reason, claim 16 overcomes the § 102(b) rejection in view of Caputo.

The method of independent claim 28 is for use in a device that is coupled to a communications channel. The method includes determining a security service to perform with a data block and generating security information to pass along with the data block. The security information identifies at least one of an encryption algorithm and an authentication algorithm to be performed by the security service. The method includes processing, in a computer peripheral device that is adapted to control communication with the communications channel, the data block according to the security information.

Claim 28 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Caputo. However, Caputo fails to anticipate independent claim 28 for at least the reason that Caputo fails to teach or suggest generating security information to pass along with a data block, which identifies one of an encryption algorithm and an authentication algorithm to be performed by a security service and processing in a computer peripheral device the data block according to the security information.

See discussion of independent claim 1 above. In particular, although a designer of Caputo's device may arguably select a particular authentication or encryption algorithm at some point during the development of the device 10, there is no teaching or suggestion that an indication of the encryption or authentication algorithm is passed along with a data block to a computer peripheral device so that the computer peripheral device performs the encryption or authentication algorithm on the data block according to the passed-along security information. Without this teaching, Caputo fails to anticipate independent claim 28.

Independent claim 33 recites a controller for controlling communications with a transport medium. The controller includes a receiving circuit and a cryptographic engine. The receiving circuit receives data and associated control information. The security control information identifies at least one of an encryption algorithm and an authentication algorithm to be performed on the data. The cryptographic engine cryptographically processes the data based on the security control information, and the cryptographic engine is a computer peripheral device.

Independent claim 33 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Caputo. See discussion of independent claim 16 above. In particular, Caputo fails to teach or suggest a receiving circuit that receives data and associated security control information, where

the security control information identifies at least one of an encryption algorithm and an authentication algorithm to be performed on the data. Additionally, Caputo fails to teach or suggest a cryptographic engine to cryptographically process data based on such security control information. Thus, for at least the reason that Caputo fails to teach or suggest the receiving circuit of independent claim 33, Caputo does not anticipate this claim.

Dependent claims 2-12, 17-20, 29-32 and 34-37 are patentable for at least the reason that these claims depend from allowable claims. Thus, for at least the reasons that are set forth above, the § 102(b) rejections of claims 1-5, 16-20 and 28-37 are in error and should be reversed.

B. Are Claims 13-15 Anticipated by U.S. Patent No. 5,268,962 (Abadi)?

The article of independent claim 13 includes a machine-readable storage medium that contains instructions for execution in a system that includes a computer peripheral device that is adapted to control communications with a communications channel. The instructions when executed cause the system to receive a data block from a computer peripheral device and determine from information in the data block if a security service has been performed on the data block by the computer peripheral device. The instructions cause the system to process the data if the security service has not been performed on the data block by the computer peripheral device.

Independent claim 13 stands rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,268,962 (herein called "Abadi"). Abadi generally discloses a computer network and a technique to exchange data packet between hosts using host-to-host encryption keys.

The article of independent claim 13 recites instructions that when executed cause a system to determine from information in a data block if a security service has been performed on the data block by a computer peripheral device and process the data block if the security service has not been performed on the data block by the computer peripheral device.

Contrary to the limitations of independent claim 13, Abadi fails to teach or suggest instructions that perform the determination and processing, recited above. In particular, the Examiner cites language from lines 61-65 in column 3 and lines 24-27 in column 4 of Abadi. The language in column 3 merely recites that two host computers transmit data packets only after the hosts agree on a host-to-host encryption key. The language in column 4 recites that before a host computer 114 can exchange data packets, the host computer 114 must first establish a host-

to-host key. However, neither the language cited by the Examiner nor any other part of Abadi teaches or suggests instructions that when executed by a system cause the system to determine from information in a data block if a security service has been performed on the data block by a computer peripheral device and process the data block if the security service has not been performed on the data block by the computer peripheral device. Therefore, for at least this reason, Abadi fails to anticipate independent claim 13.

Claim 14 recites that the storage medium contains instructions that when executed cause the system to retrieve security information that is associated with the data block and send the data block and security information to a computer peripheral device to perform the security service.

Claim 14 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Abadi. Claim 14 is patentable for at least the reason that this claim depends from an allowable independent claim. Claim 14 is patentable for the additional, independent reason that Abadi fails to teach or suggest instructions that cause a system to retrieve security information associated with a data block and send the data block and the security information to a computer peripheral device to perform a security service. In the rejection of claim 14, the Examiner cites language from line 63 of column 7 to line 3 of column 9. However, the Examiner fails to specifically point out where Abadi allegedly teaches the missing claim limitations. Thus, there is no teaching or suggestion in Abadi regarding one of the host computers retrieving security information associated with a data block and sending the data block and the security information to a computer peripheral device to perform the security service. Without this teaching, Abadi fails to anticipate claim 14 for this additional, independent reason.

Therefore, for at least the reasons that are set forth above, the § 102(b) rejections of claims 13-15 are in error and should be reversed.

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue.

Respectfully submitted,

Date: January 20, 2006

Fred G. Pruner, Jr., Reg. No. 40,779
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Ste. 100
Houston, TX 77024
713/468-8880 [Phone]
713/468-8883 [Fax]

CLAIMS APPENDIX

The claims on appeal are:

1. A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying the security service;

using a computer peripheral device adapted to control communication with the communications channel to select the security service from other security services based on the security information; and

processing, in the computer peripheral device, the data block according to the security information.

2. The method of claim 1, wherein the processing includes performing cryptographic processing of the data block.

3. The method of claim 1, further comprising:

receiving the data block from a software routine; and

routing the processed data block back to the software routine after processing.

4. The method of claim 1, further comprising:

determining if the security service can be performed by the computer peripheral device; and

if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.

5. The method of claim 1, further comprising identifying a security service according to an Internet Protocol security protocol.

13. An article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communications with a communications channel, the instructions when executed causing the system to:

receive a data block from the computer peripheral device;

determine from information in the data block if a security service has been performed on the data block by the computer peripheral device; and

process the data block if the security service has not been performed on the data block by the computer peripheral device.

14. The article of claim 13, the storage medium containing instructions that when executed causes the system to retrieve security information associated with the data block and send the data block and security information to the computer peripheral device to perform the security service.

15. The article of claim 13, the storage medium containing instructions that when executed causes the system to perform the security service on the data block.

16. A controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data and associated security control information, the security control information identifying a security service to be performed on the data; and

a cryptographic engine to select the security service from other security services based on the security control information and cryptographically process the data based on the selection, the cryptographic engine being a computer peripheral device.

17. The controller of claim 16, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

18. The controller of claim 17, further comprising a device adapted to change the contents of the storage device to update the security services information.

19. The controller of claim 18, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

20. The controller of claim 17, wherein the security services information includes security association information.

28. A method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block;

generating security information to pass along with the data block, the security information identifying at least one of an encryption algorithm and an authentication algorithm to be performed by the security service; and

processing, in a computer peripheral device adapted to control communication with the communications channel, the data block according to the security information.

29. The method of claim 28, wherein the processing includes performing cryptographic processing of the data block.

30. The method of claim 28, further comprising:

receiving the data block from a software routine; and

routing the processed data block back to the software routine after processing.

31. The method of claim 28, further comprising:

determining if the security service can be performed by the computer peripheral device; and

if not, processing the data block according to the security service in a software routine instead of the computer peripheral device.

32. The method of claim 28, further comprising identifying a security service according to an Internet Protocol security protocol.

33. A controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data and associated security control information, the security control information identifying at least one of an encryption algorithm and an authentication algorithm to be performed on the data; and

a cryptographic engine to cryptographically process the data based on the security control information, the cryptographic engine being a computer peripheral device.

34. The controller of claim 33, further comprising a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

35. The controller of claim 34, further comprising a device adapted to change the contents of the storage device to update the security services information.

36. The controller of claim 35, wherein the device is adapted to update the security services information based on a predetermined replacement policy.

37. The controller of claim 34, wherein the security services information includes security association information.